



Kauzalita a strategie v oblasti bezpečnosti





Bezpečnost

- je fenomén, hrající významnou roli pro *zajištění existence* každého referenčního objektu i jeho fungování,
- určitým nedostatkem přístupu při zajišťování bezpečnosti je *nerespektování příčinné souvislosti* jevů, způsobujících narušení bezpečnosti.

0





Kauzalita (co to vlastně je??)

- většina z nás nemá sebemenší ponětí, oč se vlastně jedná,
- je to *příčinná souvislost* představuje „jakýsi“ systém založený na kauzálních vztazích, tzn. na funkčních vztazích mezi příčinami a jejich účinky,

0





Kauzalita

- je totiž považována za společný prvek lidstva, bez ohledu na společnost či postavení a člověk se s ní setkává v každodenním životě,
- společně se zkušeností je zakotvena v myšlení a uvažování každého z nás, je tedy spojena výhradně s rozvojem lidské společnosti,

0





Kauzalita

- Má kauzalita své místo a uplatnění?
- Nejprve je nutné zmínit fakt, že bezpečnost proniká, resp. zasahuje do všech oblastí i úrovní lidské aktivity a je rovněž (jako kauzalita) spjatá s vývojem lidské společnosti.

0





Kauzalita

- Zajištění bezpečnosti v zásadě stojí na managementu rizik (aktiva, hrozby, rizika protiopatření).
- Povětšinou bývá bezpečnost vymezována s vazbou ke konkrétnímu referenčnímu objektu, což má také vliv na definici bezpečnosti, která se nepatrně liší.

0





Kauzalita

- Na bezpečnost lze nahlížet z pohledu teorie rizik, krizí a příčinných souvislostí.
- Současný přístup preferuje spíše statické pojetí bezpečnosti, tzn., že kauzalitu příliš nerespektuje, což může být vnímáno jako určitý nedostatek tohoto přístupu.

0





Kauzalita

- Příčinná souvislost událostí či jevů narušujících bezpečnost přitom mnohdy sehrává klíčovou roli při formování dalších kroků a rozhodnutí, za účelem vhodného zajištění bezpečnosti.
- Je tedy žádoucí, aby na bezpečnost bylo nahlíženo také v pojetí dynamickém, které umožňuje bezpečnost hodnotit v čase jako kauzalitu.
- Lze jí využít:
 - jak dopředně, tzn. *ve formě predikce* (sledování budoucího vývoje na základě vývojových souvislostí),
 - tak i zpětně (hledáním příčin, které mohly způsobit vznik určitého následku).

0





Kauzalita

- Pojem kauzalita vychází z latinského slova „causa“ příčina.
- Jedná se o přičinnost, což je vztah, ve kterém dochází ke vzájemné spojitosti mezi příčinou a účinkem.
- „Zákon kauzality stanoví, že každé dění má nutně alespoň jednu příčinu a je příčinou dalšího dění, přičemž stejné příčiny plodí stejné následky.“

0





Kauzalita

- Kauzalitu lze definovat jako příčinnou souvislost mezi dvěma událostmi, z nichž jedna vyvolává druhou, tedy je její příčinou.
- Jako *vztah mezi příčinou a účinkem*, tedy vztah mezi událostí, která konstituuje příčinu, a událostí, která konstituuje účinek.
- Kauzalita nepředstavuje žádnou entitu ani vlastnost, lze ji chápat spíše jako relaci.

0





Kauzalita

- Kauzalitu nelze pozorovat ani uchopit, neboť se nejedná o skutečnost mající svůj samostatný průběh.
- Jde o myšlenkový prostředek, s jehož pomocí se člověk pokouší empirickou cestou prozkoumat skutečné souvislosti a odvislosti přírodního či společenského dění.

0





Kauzalita

- Koncepce příčinnosti se může jevit pouze jako antropická, jelikož vznikla na základě činnosti člověka (v lidské aktivitě je subjekt vnímán jako původce – je tedy příčinou), což má za následek to, že člověk pak analogicky očekává vyvolání následků příčinami ve veškerém svém okolí.

0





Kauzalita

- Bezprostředně souvisí s životem člověka – s tím, jak existuje, poznává i prožívá okolní svět.
- Je spjata se vším, co se v realitě odehrává a má důležitou roli jednak v lidských aktivitách, ale i vědních oborech:
 - matematice, právu, filosofii, přírodních vědách, psychologii, medicíně, biologii, historii či jazykovědě.
- Společným znakem je především potřeba zachytit jednotlivé jevy ve vzájemných souvislostech.





Kauzalita a její chápání

- S rozvojem lidské civilizace a lidské mysli se kauzální posuzování a uvažování stávalo nástrojem k:
 - čerpání i využívání přírodních zdrojů,
 - k utváření společensky organizovaných aglomerací
 - a také k pokusům o různá vysvětlení s potřebou rozmnožovat lidské vědění.
- Kauzalita na jedné straně poukazovala na faktické i objektivní řetězení jevů a na straně druhé spoluzakládala nepostradatelnou lidskou zkušenost.

0





Soudobé pojetí

- Výstupní hodnota systému (v každém časovém okamžiku) je závislá pouze na vstupu (v každém časovém okamžiku) a jeho průběhu v minulosti. Nikoliv na hodnotách vstupní funkce v budoucnosti.
- Platí rovněž následující podmínka: *„systém je kauzální, pokud se výstup systému neobjeví dříve, než je na vstup přivedena vstupní funkce.“*





KAUZALITA V KONTEXTU ZAJIŠTĚNÍ BEZPEČNOSTI

- Teorie bezpečnosti a její rozvoj byl doposud realizován jen v rámci jednotlivých oblastí, tedy pouze ve vztahu ke konkrétnímu referenčnímu objektu, tzn. státu, objektu (budově, areálu), informačnímu systému nebo technickému prostředku.
- Tyto kategorie referenčních objektů tvoří jednotný pilíř metodologického rámce.

0





Řízení bezpečnosti dle jednotlivých oblastí

Úroveň	Charakteristika	Oblast řízení
mezinárodní, státní	politologický charakter	strategická studia
region, municipalita, podnik	havarijní plánování, ochrana obyvatelstva	krizové řízení
institute, firma, občan	ochrana majetku (aktiv)	fyzická a informační bezpečnost

0





Řízení bezpečnosti dle jednotlivých oblastí

Postupem času se objevují i nové obory a oblasti, jež vyžadují systematické zajištění bezpečnosti:

- energetická bezpečnost,
- kybernetická bezpečnost.

0





Řízení bezpečnosti dle jednotlivých oblastí

V současnosti je preferováno pojetí bezpečnosti jako **statické** (hrozba – riziko – hodnocení – opatření), které však nezohledňuje časové kritérium.

Naproti tomu **dynamické** pojetí hodnotí bezpečnost v čase jako kauzalitu (příčina – důsledek).

0





Bezpečnost

- je službou pro referenční objekt a má také podíl na vytváření příslušných podmínek pro jeho funkci, tzn. eliminace vlivu nežádoucích faktorů i připravenost ke zvládnutí těchto vlivů.

0





Základní pojmy pro kauzalitu

- **Systém** lze charakterizovat jako ohraničenou strukturu prvků a jejich vazeb, dosahující určený cíl, a to v konkrétním prostoru i čase.

0





Základní pojmy pro kauzalitu

- **Proces** (v jakémkoliv systému) bývá definován jako přeměna vstupů na výstupy.
 - Nezbytnou součástí posuzování rizik je právě popis a analýza procesů v jednotlivých systémech, a to bez ohledu na oblast posuzování.
 - *„Pro bezpečnost a řízení bezpečnosti je nutné si uvědomit, že jen řízený systém je otevřeným systémem.“*

0





Základní pojmy pro kauzalitu

- Pojem **riziko** se užívá k vyjádření míry bezpečnosti, představuje jakýsi společný prvek pro všechny systémy a může mít charakter kvalitativní i kvantitativní.

0





Základní pojmy pro kauzalitu

- **Pojem bezpečnost** – jako stav zkoumaného objektu, představuje základní kámen veškeré bezpečnostní terminologie, běžně se užívá jak v obecné mluvě, tak v řadě společensko-vědních, přírodovědných či technických oborů.
 - Synonymem tohoto pojmu je slovo **jistota** a bezpečný je ten, kdo není vystaven nebezpečí nebo je zaručený či důvěryhodný.
 - Bezpečnost se vymezuje ve vztahu k potencionálním nebezpečím (resp. hrozbám) a spadá pod jednotlivé oblasti, kde má svůj specifický název:
 - ekologická bezpečnost, vojenská bezpečnost, ekonomická bezpečnost, atd.

0





Základní pojmy pro kauzalitu

Pojem bezpečnost

- Další možná členění bezpečnosti jsou:
 - **vnitřní** (potlačování a eliminace hrozeb s původem uvnitř objektu) a **vnější** (potlačování a eliminace hrozeb, které mají původ vně objektu)
 - **na tzv. tvrdou (vojenskou) a měkkou (nevojenské hrozby, kriminalita, atd.)**
 - **kolektivní (neboli mezi jednotlivými aktéry – státy či organizacemi); v rámci celého světa je to bezpečnost globální**
 - **mezinárodní, národní, individuální**
- Podle Terminologického slovníku MV ČR je bezpečnost definována jako:
- *„Stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí.“* [

0





Bezpečnostní metriky

- Obecně metrika neboli indikátor vyjadřuje **stav** (např. kvalita či efektivnost) určitého systému a může nabývat různých hodnot. Rozlišujeme metriky:
 - kvalitativní – nečíselné vyjádření
 - kvantitativní – číselné vyjádření
- Mezi hlavní znaky metrik (ukazatelů) patří zejména:
 - jejich kvantifikovatelnost,
 - dále pak prokazatelnost a porovnatelnost stavů v rámci daného systému.
- Každá oblast bezpečnosti používá vlastní metriky (neboli ukazatele) k určení konkrétního stavu bezpečnosti, přičemž je nutné určit ekvivalentní parametr, pomocí kterého lze vyjádřit změnu stavu systému.

0





Bezpečnostní metriky

- Všechny ukazatele bezpečnosti souvisejí (ať už přímo či nepřímo) s **časem**, neboť prostřednictvím času se uskutečňuje měřitelnost jednotlivých procesů.
- Je nezbytné si uvědomit také plynutí jednotlivých stavů za sebou v časové posloupnosti, jelikož na rozhraní jednotlivých systémů nastávají problémy s **kontinuitou procesů**. Kritériem pro zachování kontinuity je následující podmínka:

čas obnovy < ztráta kritických funkcí 0





Bezpečnostní realita

- představuje objektivní stav, jehož vývoj jsme schopni popisovat abstraktními pojmy, zaznamenávat symbolickými zápisy a modelovat.
- V rámci teorie mezinárodních vztahů měl zásadní vliv jednak koncept **sekuritizace**, jenž byl koncem 90. let minulého století vytvořen tzv. kodaňskou školou a pak také konstituování oboru **sekuritologie** (nauka o bezpečnostní realitě).
- Jednotlivé aspekty vystihující podstatu i skladbu bezpečnostní reality, jsou uvedeny v následující tabulce

0





Skladba bezpečnostní reality

Skladba základních prvků	• aktéři, vztahy, prostředí • bezpečnostní vztahy mezi aktéry v určitém bezpečnostním prostředí a konkrétním čase, prostoru a situaci
Rovnováha	• jedná se o rovnovážný stav mezi bezpečností a nebezpečností • z pohledu bezpečnostní reality je převaha nebezpečnosti vnímána jako nežádoucí stav => dosažení rovnováhy
Kvantifikace	• bezpečnost i nebezpečnost jsou měřitelnými hodnotami • lze je vyjádřit z hlediska intenzity i jejich potencionální schopnosti ovlivňovat objektivní realitu. ⁰





Kodaňská škola

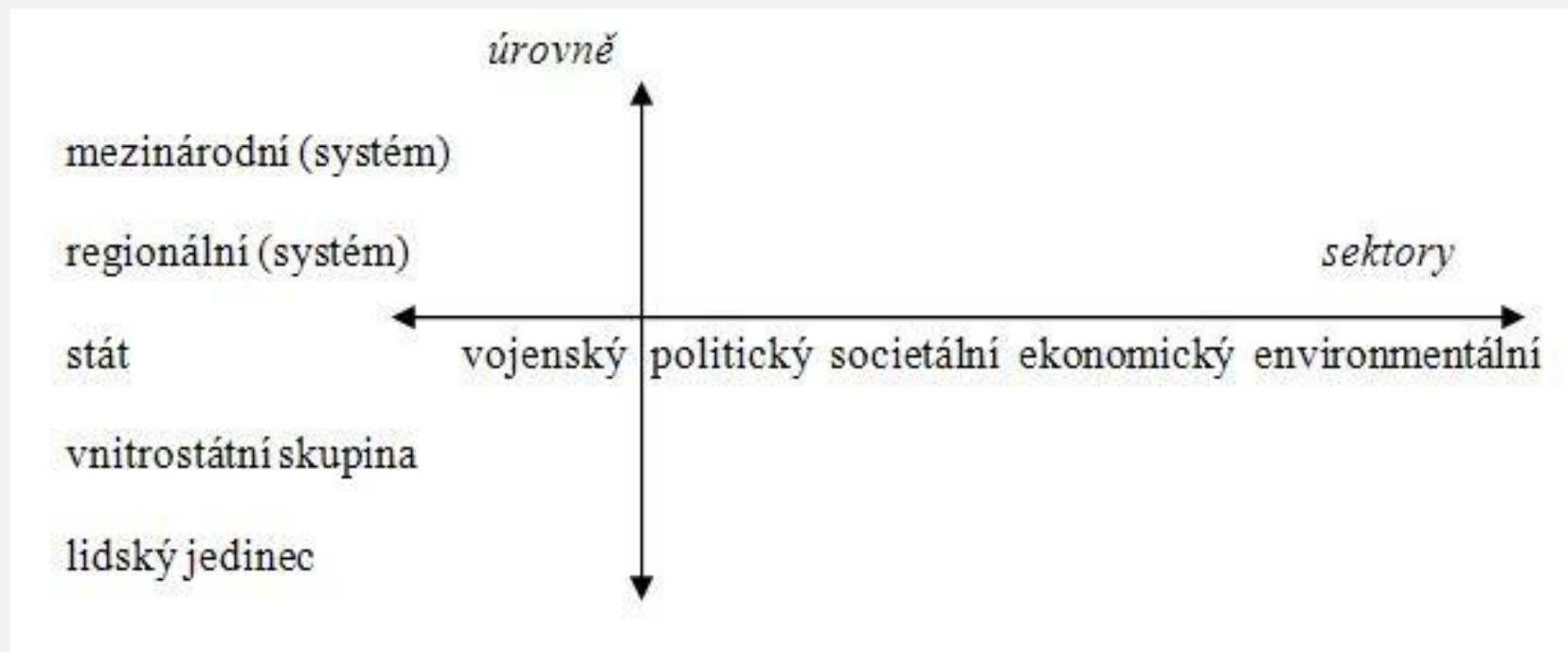
- Významným počinem v oblasti bezpečnosti je pojetí „kodaňské školy“, jejíž koncept mnohem více vyhovuje dynamice i různorodosti vývoje bezpečnostní reality oproti tradičním přístupům.
- Kodaňská škola rozpracovala teoretický rámec a s využitím sektorového přístupu vytvořila dvojdimenzionální model bezpečnosti založený na 3 okruzích zkoumání:
 - **Čí bezpečnost?** jedince, skupiny, státu, regionálního či mezinárodního systému => **vertikální osa**
 - **Bezpečnost jakých hodnot?** zkoumání vztahové nebo emocionální vazby referenčního objektu
 - **Bezpečnost před čím?** zkoumání a charakteristika hrozeb dle jejich původu => **horizontální osa**

0





Bezpečnost je výslednicí souřadnic vertikálních a horizontálních rovin, kde vertikální osa udává kvalitativní proměnu referenčního objektu a horizontální osa představuje kvalitativní odlišnost hrozeb



0





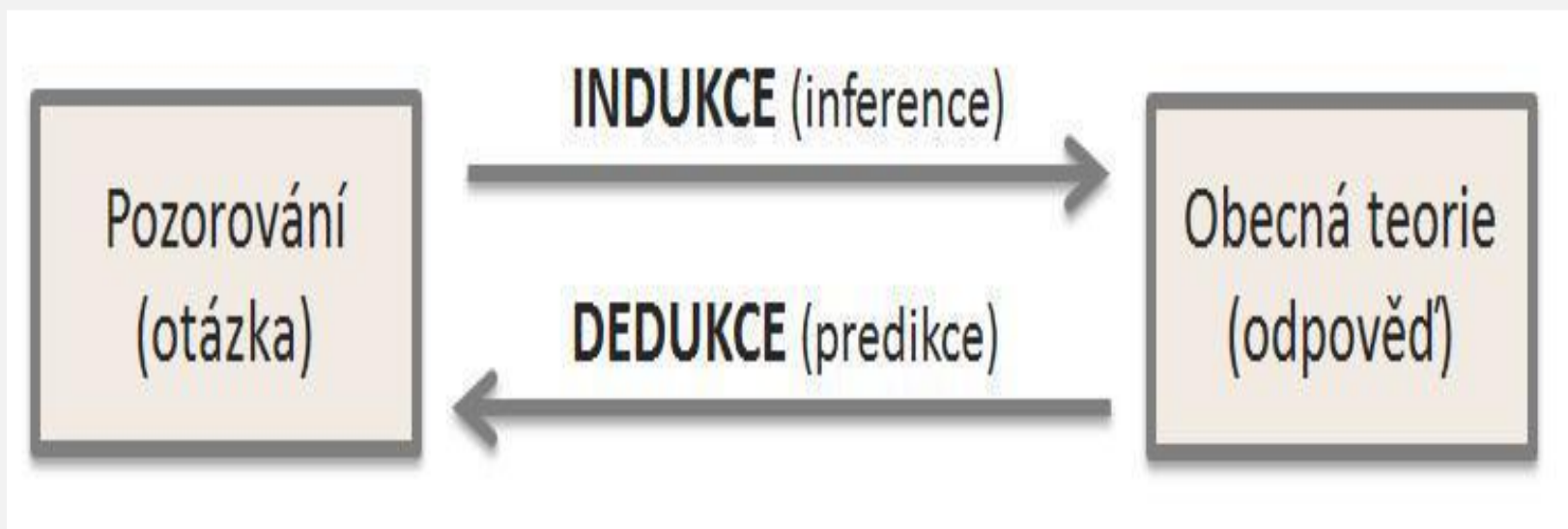
Kauzální závislost – základní pojmy a přístupy

Procesní zkoumání kauzality

- Celá řada vědních disciplín má určitou souvislost se systémovým přístupem (resp. musí být pomocí tohoto přístupu zajištěna), např.: synergetika, kybernetika, teorie systémů, atd.
- Popis kauzálních závislostí v těchto vědách má **kvalitativní** charakter (nikoliv kvantitativní).
- Vlastnosti kauzální závislosti:
 - *popis příslušného jevu v pořadí příčina – následek*
 - *funkce následnosti v čase a prostoru*
 - *popis vývoje a změn (končící děj je začátkem následujícího, neustálý vývoj)*
- Veškeré přístupy sloužící k posuzování bezpečnosti a rizik (induktivní či deduktivní) využívají, resp. pracují s příčinnou (kauzální) závislostí.

0







Deduktivní přístup

- $\Rightarrow$ od následku k příčině
- spočívá ve vyvozování nových, logicky jistých závěrů, a to na základě již známých a obecných předpokladů (premis), přičemž tyto vyvozené závěry jsou jisté,
- dedukce se využívá při hledání příčin skutkových stavů, nebo ji lze využít také k testování platnosti vyslovené hypotézy.

0





Induktivní přístup

- $\Rightarrow$ od příčiny k následku
- spočívá ve vyvození obecného závěru z dílčích poznatků, rozlišuje se indukce úplná a neúplná, která má povahu předsudku.
- slouží k nalézání podmínek výskytu konkrétního jevu, tyto podmínky však zjišťují pouze podmíněnost (nelze jimi rozlišit příčinu od účinku).

0





Základní pojmy popisující kauzální závislost

- NEBEZPEČÍ (*periculum*)
 - Jedná se o statickou vlastnost objektu systému a ve skutečnosti pojem nebezpečí představuje potenciál rizika, který se může v určitém prostoru a čase aktivovat.

0





OHROŽENÍ (*comminatio*)

- Ohrožení je typ rizika a v managementu rizik bývá označováno za potenciální nebezpečí, s tím, že může nebo také nemusí nastat. Vyjadřuje narušení běžných funkcí, vazeb a vztahů v příslušném prostoru i čase.
- Ohrožení s sebou přináší dodatečné výdaje pro organizaci, neboť je nutné zajistit ochranu před ním a tím se připravit na budoucí rizika. Kategorie ohrožení:
 - **neúmyslné poškození** – různé poruchy či selhání systémů (např. dopravních, komunikačních, informačních, atd.)
 - **selhání technického zařízení** - nedodržení různých předpisů, norem, postupů a zákonů
 - **úmyslné poškození** – různé krádeže či zhářství, podvody v daňové i Pojistné oblasti, ale také kybernetické útoky a terorismus
 - **živelná (přírodní) pohroma** - záplavy, tornáda, eroze půdy, bouřky, zemětřesení

0





HROZBA (*comminatio*)

- Libovolný jev neboli skutečnost (fenomén) mající potencionální schopnost poškodit zájmy subjektu, případně nějakou chráněnou hodnotu.
- Míru hrozby určuje jednak velikost možné škody, ale i časová vzdálenost možného uplatnění dané hrozby, přičemž časová vzdálenost bývá vyjádřena pravděpodobností, tzn. rizikem.
- Jedná se o děj, při kterém dochází k aktivaci nebezpečí (aktivní vlastnost zdroje působení). Tohoto pojmu se využívá především v oblasti politických a vojenských věd.
- Hrozby mohou být buď **neintencionální** (mající náhodnou povahu) nebo **intencionální** (jinak řečeno antropogenní, tedy zamýšlené).

0





POŠKOZENÍ (*damnum*)

- Poškození není stav, nýbrž proces a tímto pojmem lze popsat způsob, jak dospět ke škodě.
- Platí, že ne každé ohrožení může přerůst do procesu poškozování, neboť koncový stav (výsledná škoda) je podmíněn prostřednictvím opatření, jež jsou aktivovány v příslušném stavu daného prostoru.
- Vysvětlení kauzální závislosti pro popis ukončeného děje v čase nutně vede k rozlišení pojmů poškození a škoda:
 - **poškození** = *proces* (probíhající);
 - **škoda** = *stav* (ukončený)

0





ŠKODA (*damnum*)

- Tento pojem slouží pro všeobecný popis nepříznivé události, vyjadřuje stupeň (rozsah) poškození a nejčastěji se prezentuje ve formě kvantifikátoru (např. finančních ztrát).
- V praxi se škoda vyskytuje v těchto formách:
 - poškození zdraví a majetku
 - nepříznivá změna přírodního zdroje
 - v pojišťovnictví – majetková, zdravotní či finanční újma

0





DŮSLEDEK (*resultaret*)

- Pojem důsledek se používá pro popis kauzality, jedná se o koncový stav, který je reprezentovaný pojmem škoda (v oblasti popisu ztrát představuje synonymum pojmu škoda).
- Katastrofa, průmyslová či technologická havárie jakožto výsledek kauzality, jsou pouze konkrétním důsledkem s příslušnou škodou (ztrátou).
- Důsledek představuje kvantitativní nebo kvalitativní vyjádření škody či události, kterou může být:
 - poškození zdraví, životního prostředí, taktéž i materiální a finanční ztráta.

0





Vlastnosti systémů ve vztahu ke kauzalitě

- Následující pojmy popisující vlastnosti systémů jsou směrodatné pro bezpečnost i možnost změn, neboť popisované vlastnosti pak určují schopnost **adaptace**, resp. transformace systémů v konkrétním prostoru a čase.

0





ODOLNOST (*resiliencia*)

- Odolnost je důležitá vlastnost systémů a **určuje, do jaké míry systém zůstává v původním stavu**, pokud dojde k jeho zatížení (=> působení ohrožení či hrozeb).
- Odolnost může být vyjádřena také jako schopnost systému absorbovat nežádoucí energii, využít odchylky i změny a zachovat původní funkcionalitu, aniž by došlo ke kvantitativním změnám ve struktuře daného systému.
- Pojem **pružná odolnost** lze definovat jako míru rozsahu jednotlivých odchylek, které je systém schopen absorbovat, a to před přechodem z původního stavu do nového stavu se změnou funkcionality.
- Pružná odolnost tedy představuje míru schopnosti daného systému absorbovat jednotlivé změny stavu.

0





ZRANITELNOST (*Vulnerability*)

- Zranitelnost je v podstatě **schopnost systému reagovat na výskyt nežádoucí události**. Vyjadřuje stav, ve kterém systém není schopen přijímat další energii a zachovat tak svůj původní stav (funkcionalitu).
- Jedná se o stav mezi ohrožením (hrozbou) a schopností systému snížit toto ohrožení (hrozbu), a to v konkrétním čase. Zranitelnost bývá definována především pomocí dvou následujících faktorů:
 - **citlivost** neboli náchylnost ke způsobení rizika hrozbou;
 - **kritičnost**, vyjadřující význam konkrétního aktiva pro organizaci, jednotlivce či systém.

0





CITLIVOST (*sensibilitatem*)

- Citlivost je vlastnost systému udávající potencionální změnu a z pohledu zachování požadované míry bezpečnosti představuje důležitou vlastnost systému.
- Je to schopnost systému přijmout podnět zevnitř / zvenku a určuje kdy, kde a jak se systém začne měnit.
- Určuje změnu celé struktury systému, avšak této změny je možné dosáhnout i působením na jeden prvek systému, což vystihuje i následující přísloví: *„řetěz je jen tak silný, jako je silné jeho nejslabší oko.“*

0





ADAPTACE (*adaptationem*)

- Adaptace je schopnost systému **přizpůsobit se novým podmínkám**. Je to schopnost změnit se s ohledem na konkrétní ohrožení / hrozby, které působí na systém zevnitř / zvenku, a to při zachování většiny původních funkcí systému.
- „Adaptace se vztahuje na reakci na události, změněné podmínky s cílem vyhnout se nepříjemným důsledkům protireakcí.“

0





OBNOVITELNOST (*recoverability*)

- Obnovitelnost je **schopnost systému vytvořit původní funkcionalitu** a je vhodné ji řešit s ohledem na ostatní systémové vlastnosti i ekonomickou návratnost.
- Tento pojem se uplatňuje především v oblasti bezpečnosti IT a také při tvorbě plánů kontinuity.
- Důležité je si uvědomit, že plynutím času se změnil stavový prostor a je tedy otázkou, zda se dospělo k původnímu stavu či nikoliv.

0





ZMĚNY V SYSTÉMU

- Změny v systému mohou být buď postupné (*evoluční*) nebo skokové (*revoluční*). Teorie bezpečnosti zachycuje prokazatelný vztah mezi těmito pojmy:
 - **nebezpečí** reprezentuje vlastnosti prvků systému
 - **ohrožení** / **hrozba** reprezentuje vazby mezi prvky systému, a to buď jednostranné, nebo oboustranné
 - **poškození** představuje formu změn jednotlivých vazeb a prvků v systému
 - **škoda** je nový stav systému, jehož funkcionality je navenek nezměněná

0





Čas jako klíčový faktor v řízení bezpečnosti a rizik

- Nezbytným faktorem v řízení bezpečnosti i rizik, je právě **čas**. V současnosti užívané pří-stupy i metody k posuzování rizik, však tento klíčový faktor nezohledňují, a to zcela vědomě. Je tedy žádoucí, aby následující východiska k tvorbě metod pro posuzování bezpečnosti (rizik), byla v budoucnu zohledněna:
 - *příslušný prvek systému je potenciálem charakteristického ohrožení*
 - *vazba v systému vytváří ohrožení*
 - *v systému může dojít k aktivaci vazeb v čase*
 - *konkrétní ohrožení se projeví jen při konkrétní interakci v konkrétním čase*
 - *výsledná bezpečnost (riziko) je funkcí bariér a vazeb v systému*

0





VYUŽITÍ METOD KAUZÁLNÍ ANALÝZY PŘI PREDIKCI A MINIMALIZACI DOPADŮ

- Pro účely kauzální analýzy nejsou zavedeny žádné speciální metody, nýbrž se využívají již známé, osvědčené techniky z oblasti řízení rizik a tvorby predikcí.
- Jedná se o takové metody, které jsou schopny zachytit veškeré souvislosti zkoumaných událostí či jevů včetně jejich vzájemných vazeb a příčinných souvislostí.

0





VYUŽITÍ METOD KAUZÁLNÍ ANALÝZY PŘI PREDIKCI A MINIMALIZACI DOPADŮ

- Analýza příčin a následků poruch (FMEA)
- Analýza stromem poruch (FTA)
- Analýza stromem událostí (ETA)
- Analýza příčin a následků (CCA)
- Mind Maps
- Ishikawův diagram (rybí kost)
- Organizační diagnostika
- Strom významnosti

5870





VYUŽITÍ METOD KAUZÁLNÍ ANALÝZY PŘI PREDIKCI A MINIMALIZACI DOPADŮ

- Morfologická analýza
- Scénáře
- Křížové interakce
- Organizační diagnostika

5970





Analýza příčin a následků poruch (FMEA)

- analytická technika umožňující včasné identifikovat možné poruchy, chyby či vady v rámci daného systému, které by mohly ovlivnit jak jednotlivé funkce systému, tak i výslednou kvalitu a bezpečnost. Jedná se o postup, jehož podstatou je rozbor způsobů selhání i jejich důsledků, jež umožňuje hledání dopadů a příčin na základě systematicky a strukturovaně vymezených selhání zařízení.
- Použití metody FMEA vyžaduje značnou zkušenost analyzovaného systému, zejména při správné identifikaci možných vad a jejich následků. Může být provedena jedním analytikem, nicméně se doporučuje složení týmu z více lidí, aby byl zajištěn dostatek znalostí a zkušeností o daném systému. V případě složitějších systémů je možné následně provést analýzu pomocí metody FTA.
- Výstupem je kvalitativní systematický seznam jednotlivých zařízení (včetně jejich poruch) a následků s možností kvantifikace. Součástí bývá rovněž odhad nejhorších případů následků a následuje doporučení pro zlepšení úrovně bezpečnosti.

0





Analýza stromem poruch (FTA)

- **FTA** (*Fault Tree Analysis*) je **deduktivní** kauzální technika sloužící k vyhodnocení pravděpodobnosti selhání daného systému a uplatňuje se především v oblasti řízení rizik, kvality či bezpečnosti. Tato metoda se využívá v rámci složitějších systémů a obvykle následuje až po analýze metodou FMEA.
- Tato graficko-analytická metoda zachycuje různé kombinace poruch (událostí) zařízení a lidských chyb, jež mohou dospět až k hlavní systémové poruše, která se nazývá jako „vrcholová událost“ (VU). Na základě toho je zaměřena pozornost na **preventivní** a **eliminační** opatření (vztahované k relevantním primárním příčinám) s cílem minimalizovat pravděpodobnost vzniku nehody.
- Tato technika používá k analýze kombinaci Booleových logických hradel (AND a OR) v rámci poruchového modelu určitého zařízení. Metodu FTA lze aplikovat jednak pomocí **kvalitativního** přístupu (cílem je identifikace potencionálních příčin a cest vedoucích k VU), ale i **kvantitativně** (s cílem určit konkrétní pravděpodobnost VU).

0





Analýza stromem událostí (ETA)

- ETA (*Event Tree Analysis*) patří mezi induktivní kauzální analytické techniky a využívá se především k vyhodnocení průběhu procesu i událostí, které by mohly potencionálně způsobit nehodu. ETA sleduje průběh procesu, přičemž jednotlivé události jsou konstruovány na základě dvou kritérií: *příznivé* nebo *nepříznivé*. Uplatňuje se (stejně jako předchozí metody) v oblasti řízení rizik, kvality i bezpečnosti.
- Jedná se o graficko-statistickou metodu, která zobrazuje systémový strom událostí prostřednictvím rozvětveného grafu (v závislosti na počtu narůstajících událostí se výsledný graf postupně rozvětjuje). Tato metoda je vhodná především pro analýzu komplexního procesu (všechny události v rámci posuzovaného systému).
- Podstatou metody ETA je rozbor sekvence jednotlivých činností a událostí vedoucích k nehodě, přičemž jsou zohledněny i potencionální odezvy bezpečnostního systému či lidské obsluhy a výstupem jsou pak různé **scénáře nehody**.
- Cílem této metody je získat konkrétní návrhy na snížení pravděpodobnosti vzniku nehody včetně následků z ní plynoucích.

0





Analýza příčin a následků (CCA)

- **CCA** (*Cause Consequence Analysis*) je kauzální analytická technika používaná v rámci řízení rizik, konkrétně pro lepší porozumění poruchám, a to pomocí vyhodnocování pravděpodobnosti selhání systémů se zaměřením na jejich příčiny.
- Tato metoda v sobě zahrnuje, resp. kombinuje deduktivní analýzu stromu poruch (FTA) a induktivní analýzu stromu událostí (ETA). Navíc umožňuje zahrnout i časové zpoždění. CCA se uplatňuje tam, kde je potřeba snižovat poruchovost složitých systémů (v oblastech jako je např. energetika, vesmírný výzkum, letectví, jaderná energetika a další).
- Podstata metody CCA v praxi:
 - znázorňuje logiku poruchy (v časovém sledu), a to od kritické události až do koncového stavu nehody s nežádoucími následky,
 - vytváří diagramy s nehodovými sekvencemi včetně kvalitativních popisů možných koncových stavů nehod.





Mentální mapy (Mind Maps)

- Představují účinnou analytickou techniku, která se využívá při řešení problémů, učení i osobním rozvoji. Jedná se o grafické znázornění řešeného problému formou grafů, které zahrnují všechny aspekty řešeného problému včetně jejich vzájemných vazeb. Mapy se vytvářejí buď ručně na papír nebo pomocí speciálního softwaru na PC.
- Této metody lze využít i ke kauzální analýze kauzalitou, jelikož je schopná zaznamenat řetězení příčinných souvislostí mezi zkoumanými jevy (událostmi).
- Metoda je aplikovatelná jak **deduktivně** (od následku k příčině), tak **induktivně** (od příčiny k následku).
- Výhody:
 - přehlednost a **univerzálnost** (mentální mapy lze využít v jakékoliv oblasti řízení),
 - možnost skupinového využití (např. v rámci brainstormingu),
 - možnost úprav a dodatečných změn (platí v případě elektronického zpracování)

0





Ishikawův diagram

- Princip diagramu Ishikawa vychází z „jednoduché kauzality“ - každý následek (problém) má svou příčinu nebo kombinaci příčin. Jedná se o jednoduchou analytickou techniku, je-jímž cílem je určit nejpravděpodobnější příčiny řešeného problému.
- Přezdívá se mu také diagram **rybí kosti**, neboť svým tvarem připomíná rybí páteř. Jednotlivé části páteře jsou tvořeny několika oblastmi, do kterých jsou poté řazeny potenciální příčiny definovaného následku. Tento následek bývá v diagramu vyznačen většinou na pravé straně (v místě rybí hlavy) a pomocí dedukce se postupuje směrem doleva, tedy od následku až ke konkrétním příčinám.
- Využití Ishikawova diagramu v praxi:
 - vzhledem ke své univerzálnosti nachází Ishikawův diagram uplatnění v oblasti kvality při hledání příčin nekvality, ale také v oblasti rizik či řešení problémů.
 - často je používán při týmových technikách hledání řešení, jako je např. brainstorming.
 - při řešení problému se v diskusi nebo pomocí jiné analytické techniky systematicky hledají jeho možné příčiny a znázorňují se formou rybí kostry.
 - Ishikawův diagram je možné použít jak **zpětně** pro hledání příčiny problému, tak **dopředně** při návrhu výrobku pro preventivní určení a eliminaci příčin produktů.

0





Ishikawův diagram

- V rámci této techniky se uplatňují metody 8M, 6M či 5M, které jsou směrodatné pro sestavení diagramu, neboť udávají jaké oblasti (i počet oblastí) budou sloužit k utřídění jednotlivých příčin zkoumaného problému.
- Tyto metody se volí na základě charakteru řešeného problému, složitosti procesu i v závislosti na požadovaném účelu a cíli.

0





Metoda 8M

- Příčiny se většinou hledají v základních dimenzích - následující seznam uvádí 8 typických dimenzí používaných ve výrobě (**8M**).
 - Man power - People (Lidé) - příčiny způsobené lidmi
 - Methods (Metody) - příčiny způsobené pravidly, směrnicemi, legislativou či normami
 - Machines (Stroje) - příčiny způsobené zařízením (stroje, počítače, nářadí, nástroje)
 - Materials (Materiál) - příčiny způsobené vadou nebo vlastností materiálů
 - Measurements (Měření) - příčiny způsobené nevhodným měřením
 - Mother nature - Environment (Prostředí) - příčiny způsobené vlivem prostředí - teplo-tou, vlhkostí, nebo také kulturou
 - Management - příčiny způsobené nesprávným řízením
 - Maintenance - příčiny způsobené nesprávnou údržbou

Existuje také metoda **5M**, **6M**, které jsou zkrácenou verzí metody **8M**.

0





Organizační diagnostika

- Je **deduktivní** metoda, která se využívá výhradně pro účely v rámci organizace. Primárně má za úkol odhalovat potencionální problémy v organizaci (včetně posuzování jejich významu) a poté navrhnout konkrétní postup řešení.
- Důraz je kladen především na včasné odhalení problémů a rychlost odezvy při jejich řešení => cílem metody je tedy **prevence**. Běžně se užívají následující metody a techniky:
 - studium dokumentů,
 - dotazování,
 - vyhodnocování a modelování.
- Bez patřičných informací, znalostí a pochopení funkčních vztahů (v rámci konkrétní organizace) není možné získat finální řešení problému, které by zároveň bylo objektivní a věrohodné. Provedení kauzální analýzy se v tomto případně jeví jako neadekvátnější řešení, neboť systematicky nachází jednotlivé řetězce příčin a následků.
- Organizace je chápána jako systém (včetně vzájemných vazeb), přičemž předností kauzální analýzy je její komplexní vnímání jakéhokoliv systému a tím pádem nehrozí to, že by nějaký prvek či vazba byly opomenuty. Postup při provádění kauzální analýzy je následující:]
 - popis problému (identifikace, lokalizace, čas, rozsah)
 - specifikace rozdílů a odlišností (co je a co není problém)
 - specifikace změn (předpokládané příčiny problému)
 - testování příčin a jejich verifikace

0





Strom významnosti

- Strom významnosti představuje analytický postup, který využívá k zápisu hierarchickou strukturu ve formě stromu. Tato struktura znázorňuje prvotní problém, který postupně rozčleňuje na jednotlivá témata (díličí podtémata).
- Výstupem je vizuální prezentace ve formě hierarchické struktury dané oblasti, znázorňující detailní aspekty řešeného problému. Tato metoda se využívá hlavně v rámci normativní prognostiky.
- Postup je následující:
 - Stanovení obecného cíle (budoucí stav),
 - Identifikace potřeb nebo technických možností k dosažení cíle,
 - Identifikace prostředků,
 - Konstrukce stromu významnosti, (postupuje se od více abstraktního k detailům, položky jsou řazeny dle významnosti a jednotlivé větve stromu představují rozhodovací úrovně (alternativní způsoby řešení situace).
 - Určení významnosti jednotlivých položek (podklad pro rozhodování).

0





Morfologická analýza

- Používá se jako podpůrná metoda ke stromu významnosti se a její podstata je následující:
 - zahrnuje mapování zájmového problému s cílem získání širšího nadhledu nad možnými způsoby jeho řešení,
 - nalézá možné kombinace řešení,
 - morfologie = učení o tvaru, formách, vnější a vnitřní skladbě zkoumaného objektu,
 - spočívá ve vytvoření matice, která obsahuje všechny faktory ovlivňující řešení,
 - kombinace získané z matice pak budou obsahovat různá řešení dílčích problémů a tím vytvářet komplexní varianty řešení.

0





Křížové interakce

- Je metoda, jejímž cílem je výpočet pravděpodobnosti výskytu určité události na základě známých pravděpodobností výskytu jiných událostí, které mohou ovlivnit vznik události sledované. Vzájemné vztahy mezi takovými událostmi se nazývají **křížové interakce**.
- Tato metoda upozorňuje na vzájemné řetězení příčinných souvislostí mezi událostmi (někdy se hovoří o tzv. **domino efektu**) a umožňuje rovněž odhadnout, jakým způsobem ovlivní určitá změna (politika, trend, atd.) pravděpodobnost výskytu ostatních událostí. Počáteční i podmíněné pravděpodobnosti stanovují experti a postup je následující:
 - vytvoří se seznam událostí,
 - těmto událostem se určí počáteční pravděpodobnosti jejich vzniku v budoucnosti,
 - dále se vytvoří matice událostí,
 - pro každou kombinaci událostí se určí limity podmíněných pravděpodobností,
 - v posledním kroku se vypočítají rozpětí podmíněných pravděpodobností.

0





Scénáře

- **Scénář** = jedna z forem zpracování prognózy, jenž popisuje průběh možného budoucího vývoje v konkrétním *časovém pásmu*. Scénáře nemají za úkol přesně predikovat budoucí vývoj, nýbrž jen popsat vývojové souvislosti mezi jednotlivými událostmi (tyto události stanovuje většinou autor). Scénáře se uplatňují zejména při tvorbě koncepcí a strategií.
- Nejčastěji se scénáře dělí do tří kategorií: **prediktivní**; **explorační**; **normativní**
- Příčinná souvislost je zde jasně prokazatelná, neboť vývojové souvislosti nejsou nic jiného než systematicky utvářený kauzální řetězec (směrem) do budoucnosti. Současné události lze chápat jako příčiny dalších událostí, které zase ovlivní či zapříčiní vznik jiných událostí, atd. Konkrétní události (příčiny) jsou voleny v závislosti na požadovaných cílech, na základě požadavků zadavatele, splnění daného účelu, apod.
- Příprava
 - stanovení zkoumané oblasti a její ohraničení,
 - charakteristika zkoumané oblasti,

0





Scénáře

- Tvorba scénářů:
 - stanovení hybných sil v dané oblasti včetně jejich popisu (např. ekonomický růst, atd.)
 - definování událostí, které ovlivňují hybné síly a mění řetězce příčin a následků
 - projektování hybných sil – nutností je vymezit souvislosti, dynamiku či vliv možných událostí (např. pomocí metody analýzy dopadů trendů)
 - příprava jednotlivých scénářů – vychází z kvantitativních prognóz hybných sil; díky nim začínají být zřejmé řetězce příčin a následků možných událostí
- Zpravodajství a využití scénářů:
 - dokumentace (text, grafy, tabulky....)
 - vymezení důsledků zpracovaných alternativních scénářů,
 - testování politik – ke každému scénáři je možné vytvořit politické strategie a ty pak kvantitativně testovat

0





Použití kauzálních metod při řešení bezpečnostního incidentu

- **Bezpečnostní incident (zkráceně BI) je pojem, který označuje nějakou nestandardní či nepříjemnou bezpečnostní událost, která vyúsťuje k narušení pravidel bezpečnosti v rámci organizace.**
- V důsledku takové události může dojít k různým problémům (ke katastrofě, nehodě či finanční ztrátě), což může způsobit zvýšení rizika i snížení bezpečnosti.
- V praxi je řešení BI součástí správně nastavených procesů v oblasti bezpečnosti. Vznik BI souvisí se selháním bezpečnostních opatření či porušením bezpečnostní politiky a dle jeho povahy se rozlišuje:
 - informační BI - narušení důvěrnosti, celistvosti a integrity informace
 - personální BI - narušení osobního bezpečí
 - BI fyzické povahy - narušení bezpečí fyzického majetku (např. vloupání)
- Za bezpečnostní incident se často považuje i podezření na porušení bezpečnostní politiky

0





Použití kauzálních metod při řešení bezpečnostního incidentu

- Za bezpečnostní incident se často považuje i podezření na porušení bezpečnostní politiky nebo pokus o překonání bezpečnostních opatření.
- Bezpečnostní incident má obvykle následující průběh:
detekce incidentu – analýza incidentu – reakce na incident.





Praktické využití kauzality k řešení bezpečnostního incidentu

- Pomocí metod analýzy kauzality nelze řešit všechny BI, ale pouze ty, které se projevují určitou kauzální závislostí, tedy jsou ve vztahu příčina – následek.
- Existují dva možné přístupy k provádění kauzální analýzy, a to **deduktivní** (zpětné hledání příčin, které způsobily vzniklý následek) nebo **induktivní** (na základě současných okolností se zjišťuje možný budoucí následek).

0





Praktické využití kauzality k řešení bezpečnostního incidentu

- Důležité je také rozlišit událost od incidentu, aby byly zvoleny vhodné nástroje a postupy k jejich řešení:
 - **bezpečnostní incident** = to, co se již odehrálo a zapříčinilo narušení nebo selhání bezpečnosti (někdy i vícekrát).
 - **bezpečnostní událost** = je i to, co přímo nezapříčinilo narušení či selhání bezpečnosti, avšak mohlo by (je nutné najít příčinu a odstranit ji).

0





Bezpečnost a strategie

- Tyto pojmy jsou vzhledem k momentálnímu dění v České republice i ve světě stále více skloňovány.
- Obecná definice pojmu bezpečnostní strategie není v odborné literatuře uváděna, můžeme se dočíst pouze o **bezpečnostní strategii České republiky, státu, firmy** a podobně.

0





Bezpečnost a strategie

- Význam slova **strategie** můžeme definovat jako **koncepční organizaci a řízení určité činnosti** za účelem ovlivnění budoucích podmínek a dosažení definovaných cílů.

0





Bezpečnost a strategie

- **Strategie** bývá chápána jako obecný postup či umění **konceptně dosahovat stanovených cílů** pomocí identifikovaných prostředků, metod a nástrojů v určitém časovém rozvrhu.

0





Bezpečnost a strategie

Taktika označuje:

- způsob vedení a promýšlení určité činnosti v konkrétní situaci,
- volbu dílčích prostorově a časově omezených postupů, které jsou implikovány a determinovány obecnými principy a cíli ve shodě se strategiemi či strategickými koncepcemi v dané oblasti či problematice.

0





Bezpečnost a strategie

- Pojem bezpečnost má více významů.
- Nejčastěji označuje stav, kdy **referenčnímu objektu nehrozí neakceptovatelná újma**, a také soubor opatření, kterým se v případě expozice hrozby tohoto stavu dosahuje.

0





Bezpečnost a strategie

- **Cílem bezpečnosti** jako oboru je zabránit vzniku újmy nebo minimalizovat pravděpodobnost vzniku a velikost újmy ve vybraných oblastech.
- **Újma představuje** pro referenční objekt **nežádoucí negativní projev**, který omezuje naplňování cílové funkce nebo může vést až k jeho zmaru.

0





Bezpečnost a strategie

- **(Proti) opatřeními** lze vzniku újmy zabránit a tím se vyhnout možným dopadům, s újmou spojeným.
- **Zvládání rizik** znamená bránit vzniku neakceptovatelné újmy.

0





Role bezpečnostní strategie

- Z výše uvedených definic tedy vyplývá, že rolí bezpečnostní strategie je identifikace budoucích bezpečnostních rizik a hrozeb a také změn ve vývoji referenčního objektu, které ho mohou ohrozit, a stanovení cílů a konkrétních kroků pro zajištění jeho bezpečnosti.

0





Role bezpečnostní strategie

- Jednoduše řečeno, **pokud bude kladen důraz na to, co v budoucnu může nastat a co může referenční objekt ohrozit, mohou se podnikat kroky k tomu, aby tyto nebezpečné situace nenastaly.**
 - ať už na životech, zdraví, ztrátě, zničení nebo odcizení majetku, nebo ohrožení státní svrchovanosti a územní celistvosti, ohrožení životního prostředí a podobně
- **Pokud by ale nastaly, bude se vědět, jak je možné se na ně připravit, umět jim čelit a jak je umět vládnout.**

0





Obsah bezpečnostní strategie

Každá bezpečnostní strategie by měla obsahovat následující body:

- shrnutí **aktuálního** stavu bezpečnosti daného referenčního objektu,
- **analýza bezpečnostních rizik a hrozeb,**
- **návrh opatření** k minimalizaci rizik.

0





Obsah bezpečnostní strategie

Riziko

- by se dalo charakterizovat jako **jev, událost, proces, nebo činnost**, který vzniká s určitou pravděpodobností, a zároveň má **negativní následek**.
- nelze mu přiřadit čas, ale pro potřeby modelování mu lze obecně přiřadit místo, objekty a subjekty.
- je vlastnost hrozby a má dva parametry:
 - **míru neurčitosti**, která je charakterizována pravděpodobností vzniku jevu, události, procesu, nebo činnosti,
 - **velikost nebezpečnosti**, která je charakterizována možnými následky na osoby, zvířata, majetek, kritickou infrastrukturu a životní prostředí.

0





Obsah bezpečnostní strategie

- **Hrozba je hrozivá blízkost něčeho zlého** (tedy jevu, události, procesu), který svými projevy, faktory, intenzitou a následky **omezuje, ohrožuje, ničí, devastuje a likviduje** životy, zdraví, majetek, životní prostředí, či kulturní hodnoty.
- Hrozba existuje neustále.
- Riziko definuje, s jakou pravděpodobností dojde k naplnění hrozby.

0





Obsah bezpečnostní strategie

Hrozba působí neustále a lze ji rozlišit na tři fáze:

- **existence hrozby** – ví se o existenci jevu, události, procesu, nebo činnosti, ale v daném okamžiku je hmota, síly a energie v rovnováze, pouze může dojít k určitým deformacím, výkyvům, anomáliím, kolísání hmot, sil a energií,
- **působení hrozby** – vznikla mimořádná událost, nebo krizová situace, je narušena rovnováha hmot, sil a energií jejich akumulací, či úbytkem, nebo došlo k expanzi nárůstu a k neřízenému uvolnění, nebo neřízené, náhlé regresi, či úbytku hmot, sil a energií,
- **zánik hrozby** – fyzikální, chemické, biologické, informační nebo jiné hrozby přestávají působit. Dochází k odstraňování deformací a adaptaci hmot, sil a energií po jejich uvolnění, či úbytku, je obnovována rovnováha hmot, sil a energií a vzniká nová rovnováha hmot, sil a energií.

0





Roviny zajištění bezpečnosti

Zajištění bezpečnosti lze rozdělit do tří kategorií podle typu referenčního objektu:

- na úrovni státu,
- na úrovni skupiny států,
- na úrovni organizace.

0



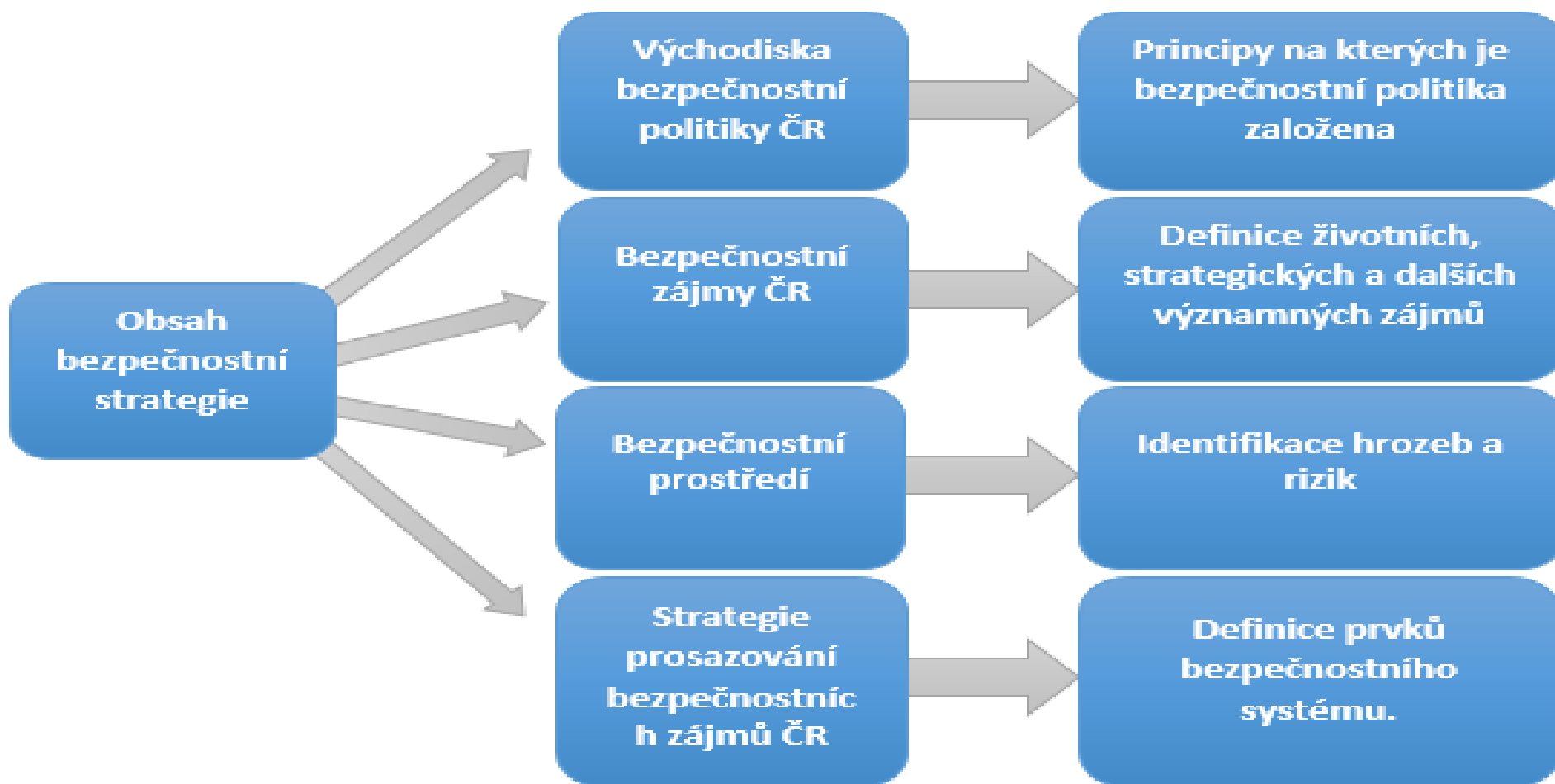


Bezpečnost organizace

- **Systém řízení bezpečnosti** v organizaci velmi úzce souvisí s řízením rizik a je zaměřeno na vytvoření takových podmínek, která pomohou předcházet nebo minimalizovat rizika pomocí různých metod, procedur, směrnic, standardů a nástrojů.
- **Cílem řízení bezpečnosti** je zajistit bezpečný provoz a zamezit bezpečnostním rizikům a hrozbám, jako jsou ohrožení či poškození života a zdraví nebo hmotných a nehmotných aktiv organizace.
- Dokument, ve kterém jsou identifikována rizika a hrozby a opatření jak jim předcházet, se nazývá **bezpečnostní strategie** organizace.

0





0





Bezpečnostní zájmy

- ČR rozlišuje své bezpečnostní zájmy podle stupně důležitosti. V Bezpečnostní strategii jsou zájmy rozděleny do tří kategorií:
 - **Životní zájmy** patří mezi nejdůležitější, především proto že se jedná o:
 - zajištění existence ČR, její suverenity, územní celistvosti a politické nezávislosti,
 - obranu demokracie a právního státu a ochranu základních lidských práv a svobod obyvatel.
 - Životní zájmy zabezpečuje stát rozsáhlými opatřeními bezpečnostní strategie, kterou provádí pomocí zahraniční, obranné a hospodářské politiky a politiky v oblasti vnitřní bezpečnosti a veřejné informovanosti.

0





Bezpečnostní zájmy

- **Strategické zájmy**

- Uskutečňování strategických zájmů je úzce spjato s ochranou životních zájmů.
- Napomáhají k zajištění společenského rozvoje a prosperity ČR.
- Mezi strategické zájmy řadíme především bezpečnost a stabilitu nejen v ČR, ale i v euroatlantickém prostoru.
- Důležitá je též prevence a zvládání místních a regionálních konfliktů a zmírňování jejich následků.
- Pro ČR je do budoucna důležité členství v mezinárodních organizacích, posilování soudržnosti a efektivnosti NATO a EU a naplňování strategického partnerství mezi NATO a EU, včetně posilování jejich spolupráce v rámci obranných a bezpečnostních schopností.
- Stejně tak rozvíjení role OBSE v oblasti prevence ozbrojených konfliktů, demokratizace a posilování vzájemné důvěry a bezpečnosti.
- Strategické zájmy se též zaměřují na spolupráci s partnerskými zeměmi v oblasti mezinárodní stability.
- Zaměřují se na ochranu demokracie, základních svobod a principů právního státu a také na zajištění vnitřní bezpečnosti a ochrany obyvatelstva, stejně jako na zajištění ekonomické bezpečnosti ČR a posilování konkurenceschopnosti ekonomiky.

0





Bezpečnostní zájmy

- **Další významné zájmy**

- Účelem prosazování dalších významných zájmů je přispět k zajištění životních a strategických zájmů ČR a zvyšovat odolnost společnosti vůči bezpečnostním hrozbám.
- Mezi další významné zájmy zejména patří:
 - snižování kriminality,
 - posilování zpravodajské ochrany a obrany ČR,
 - potlačování extremismu a jeho příčin,
 - zvyšování efektivity a profesionality státních institucí a soudnictví,
 - rozvoj občanských sdružení a nevládních organizací působících v oblasti bezpečnosti nebo ochrany životního prostředí.

0





Charakteristika bezpečnostního prostředí

- Bezpečnostní prostředí lze označit jako pojem, zahrnující jak přírodní, tak společenskou stránku reality.
- Zabývá se možnými ohroženími a zranitelností zkoumaného prostředí.
- **Bezpečnostní prostředí je jak vnější, tak vnitřní, ovlivňující bezpečnost státu.**
 - U **vnějšího bezpečnostního prostředí** jde o prostor nacházející se vně státních hranic ČR, ve kterém se realizují a střetávají zájmy ČR se zájmy jiných aktérů mezinárodních vztahů a v němž se odehrávají procesy, které mají významný vliv na úroveň bezpečnosti ČR. Události odehrávající se v prostředí mimo území ČR se pak přímo i nepřímo promítají do prostoru ČR.

0





Charakteristika bezpečnostního prostředí

- **Bezpečnostní prostředí je jak vnější, tak vnitřní, ovlivňující bezpečnost státu.**
 - Prostor na území ČR považujeme za **vnitřní bezpečnostní prostředí**. Působením na dané podmínky lze dosáhnout minimalizaci rizik, zabránění vzniku nežádoucích událostí, omezení jejich negativních dopadů, včetně rekonstrukce následků způsobených případnou nežádoucí událostí. Potřeba prognóz zde vyvstává do popředí, protože v této oblasti je důležité vytvoření představy o bezpečnostním prostředí v budoucnosti a na jejím základě, protože není jednoznačně determinována a vychází ze subjektivních pohledů, ji lze určitým způsobem ovlivňovat, nebo se na ni připravit.

0





Hrozby a rizika pro ČR

- Bezpečnostní strategie v souvislosti s charakterizací bezpečnostního prostředí používá dva základní pojmy:
 - hrozbu jako vnější fenomén s potenciálem poškodit zájmy ČR,
 - riziko jako pravděpodobnost vzniku událostí, považované z bezpečnostního hlediska za nežádoucí,
 - ekonomické.
- Mezi současné nejzávažnější hrozby pro ČR patří teroristé, teroristické skupiny a hnutí. Ti působí nejen lokálně, ale i globálně a koordinovaně. Ve spojení s extremistickými skupinami a v kombinaci se snahou o získání zbraní hromadného ničení vytváří pro ČR hrozbu strategického významu.
- Používají asymetrickou strategii, což znamená, že se vyhýbají přímému střetu. Za objekty útoku si vybírají převážně civilní cíle především ve městech, používají prostředky hromadné destrukce, usilují nejen o získání zbraní hromadného ničení, ale i nově vyvíjené druhy zbraní.





Hrozby a rizika pro ČR

- Dalšími hrozbami jsou nestabilita a regionální konflikty v euroatlantickém prostoru a jeho okolí, oslabování mechanismu kooperativní bezpečnosti, migrace nebo extremismus. Lze identifikovat typy možných konfliktů, které mají potenciál vyústit do ozbrojených střetů:
 - etnické,
 - teritoriální,
 - politické,
- V době kdy je svět takřka závislý na IT se stále zvyšuje také hrozba kybernetických útoků. Bezpečnostní strategie též zmiňuje mezi hrozbami ohrožení funkčnosti kritické infrastruktury, přerušení dodávek strategických surovin, energie nebo také organizovaný zločin.
- Hrozby mohou mít také přírodní a antropogenní původ. Nežádoucí stav mohou způsobit extrémní výkyvy počasí. U antropogenního původu jde především o infekční nemoci s pandemickým potenciálem.

0





Pokud řešíme strategii musíme vzít v potaz:

- Pokud se zaměříme na význam slova strategie, vyplyne nám skutečnost, že bezpečnostní strategie ČR ne zcela naplňuje význam tohoto slova.
- Je velmi obecná a i když jsou v ní uvedeny cíle, kam by měla ČR ve snaze zajistit svoji bezpečnost směřovat, nejsou v ní uvedeny konkrétní kroky, jak toto zajistit.
- Je určitě důležité zabývat se budoucností bezpečnostní situace ČR, nicméně dle mého názoru by bylo možné vyhotovit efektivnější výstup v rámci postupů pro dosažení stanovených cílů.
- Bezpečnost ČR je z velké části závislá také na okolních státech a společenstvích, kterých je členem, což nese pozitivní, ale i negativní důsledky.
- V případě možného mezinárodního konfliktu bychom se sami těžko bránili. Proto je pro ČR přínosem společenství v mezinárodních organizacích. V rámci společenství se ale musíme podřizovat a přijímat nastavená pravidla, což nemusí být vždy v absolutní shodě s našimi záměry a myšlenkami.

0





BEZPEČNOSTNÍ STRATEGIE ORGANIZACE

- Bezpečnost je stav, kdy je velikost všech rizik v organizaci na akceptovatelné úrovni.
- Nástrojem pro zajištění bezpečnosti je bezpečnostní systém.
- Firmy musí chránit svůj majetek a dbát na bezpečnost svých zaměstnanců.
- Dnes je také samozřejmostí, že veškeré důležité informace, se kterými organizace pracují, jsou převáděny do digitální podoby a firmy by se bez svých informačních systémů a sítí jen těžko obešly.
- Tato skutečnost je ale spojena s možnými bezpečnostními riziky. Proto by v každé firmě měla být vypracována souhrnná bezpečnostní strategie, která upozorní na konkrétní bezpečnostní hrozby a rizika a povede k za-jistění ochrany majetku, osob, zaměstnanců, jejich zdraví, ochrany dat a samozřejmě také kontinuity podnikání.

0





Bezpečnostní strategie a bezpečnostní politika

- Bezpečnostní strategie je základní dokument celkového zabezpečení organizace.
 - Umožňuje koncepční a konzistentní budování a zajištění bezpečnosti v organizaci.
 - Tento dokument v obecné rovině popisuje cíle organizace v oblasti jejího zabezpečení a konkrétní kroky jak jich dosáhnout.
- V zájmu vedení firmy pak musí být prosazování bezpečnostní politiky vyplývající ze strategie a všech jejích částí.
- Účelem těchto bezpečnostních činností je nastolit fungující bezpečnostní politiku a udržovat požadovanou míru fyzické, informační, požární i personální bezpečnosti a BOZP, v celé firmě všemi zaměstnanci i externími subjekty.

0





Otázky zajištění bezpečnosti

Bezpečnostní strategie organizace musí odpovědět na tyto otázky:

- Jaké jsou cíle organizace v oblasti ochrany aktiv?
- Jaká aktiva musí být chráněna?
- Jaká je cena těchto aktiv?
- Kdo za ně nese zodpovědnost?
- Jaká opatření budou efektivní?
- Jak bude jejich dodržování vynuceno, jaká penalizace bude za jejich nedodržení?
- Kdy a jak bude Bezpečnostní strategie zavedena do praxe?
- Jaký je cílový stav bezpečnostního systému?
- Jak a které osoby budou proškoleny?
- Jak zajistit osobní odpovědnost zaměstnanců?

0





Bezpečnostní systém organizace

- Bezpečnostní systém se vyznačuje dynamikou a vliv na něj mají různé proměnlivé činitele zasahující do procesů, které v něm probíhají.
- Tito činitelé mohou působit jak zevnitř, tak z vnějšího prostředí.
- Společným faktorem změn pro většinu bezpečnostních systémů je zejména právní rámec, ve kterém působí, protože způsob ochrany bezpečnostních zájmů organizace musí být vždy v souladu s pravidly danými právním řádem.
- K zajištění optimální funkce bezpečnostního systému je zapotřebí, aby v jeho životních cyklech byla udržována rovnováha mezi dynamikou systému ovlivňovaného nestálými podmínkami, na straně jedné a potřebou zachování jeho účinnosti nebo efektivnosti, na straně druhé.





Bezpečnostní systém organizace

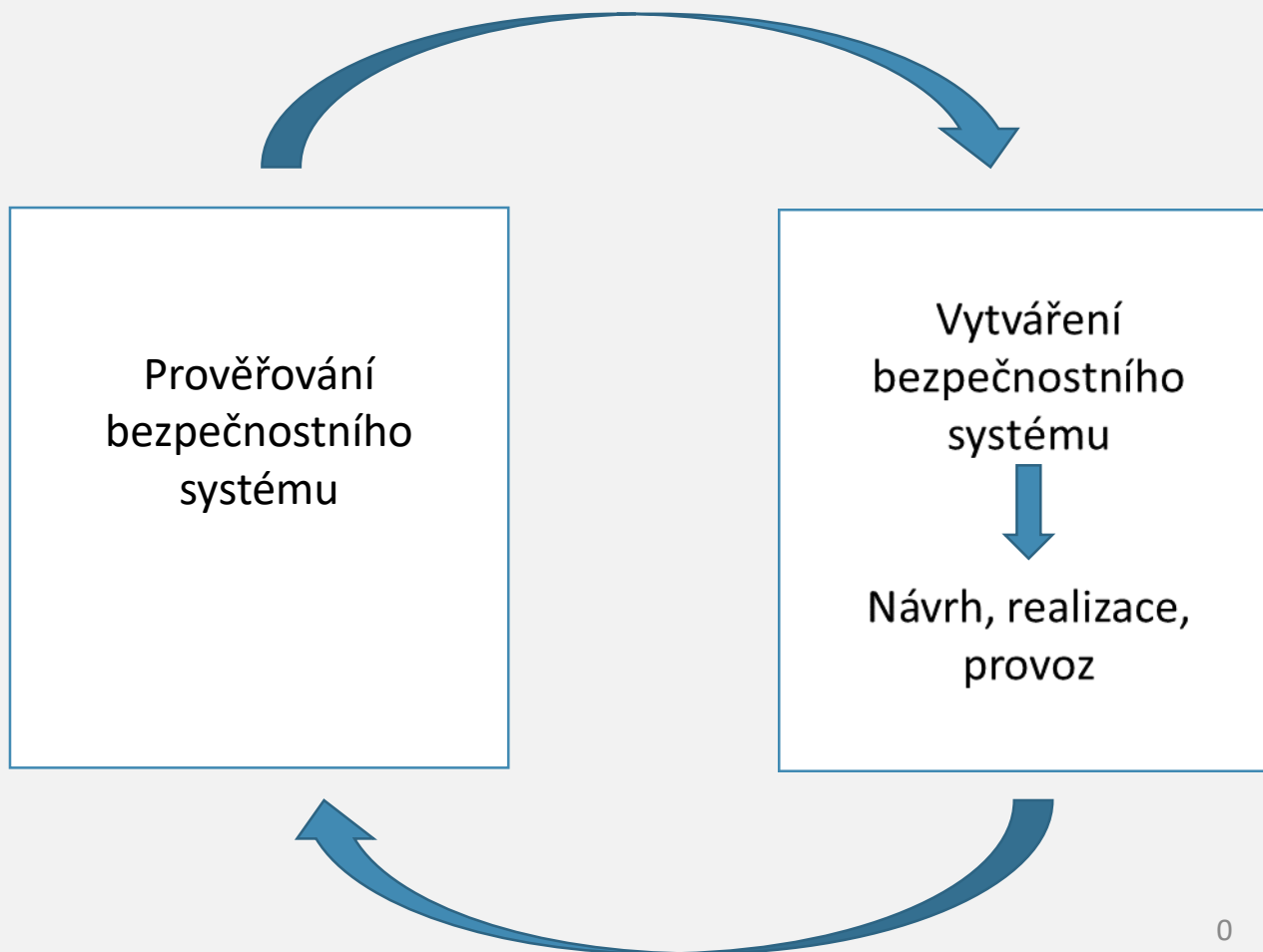
- Řízení bezpečnostního systému proto vyžaduje dohled nad procesy, které v něm probíhají.
- Jedním z velmi účinných nástrojů k trvalému udržování efektivnosti a účinnosti bezpečnostního systému je jeho systematické prověřování, na základě něhož by měly být prováděny potřebné kvalifikované a systémově orientované korektury.
- Prověřování proto musí být součástí životního cyklu bezpečnostního systému. Cyklus, který se řídí obecnými principy řídicího cyklu, má dvě základní fáze.

0





ŽIVOTNÍ CYKLUS BS



0





Kontrola způsobu zajištění bezpečnosti

- Způsob prověřování bezpečnostního systému můžeme zajistit například pomocí:
 - dozoru,
 - posouzení,
 - kontroly,
 - revize nebo
 - bezpečnostním auditem.

0





Kontrola způsobu zajištění bezpečnosti

- Bezpečnostní kontrola je jedním z neúčinnějších způsobů prověřování bezpečnostního systému organizace.
 - Ověřuje totiž nejen funkčnost systému ale i správnost jeho nastavení v organizaci, což znamená soulad s obecně závaznými předpisy a dosažení optimalizace rizik.
 - Kontrolu bezpečnosti lze provádět pouze tam, kde již existuje nějaký bezpečnostní systém. Kontrola vyhodnotí současný stav systému z hlediska shody s bezpečnostními standardy.
 - Jejím účelem je především předcházet chybám a teprve v druhé řadě napravovat chyby, které již nastaly.
 - Zaměřuje se tedy na prevenci systémových nedostatků a na jejich vyhledávání ve stávajícím systému bezpečnosti podniku.

0

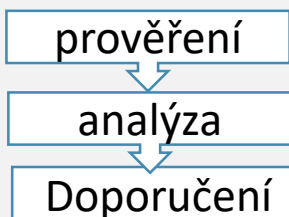




Průběh bezpečnostní kontroly

- Průběh bezpečnostní kontroly se řídí principy organizačního cyklu v obecném smyslu.
- Prověření probíhá shromážděním všech dostupných údajů známými metodami, jako:

- pozorování,
- seznámení s dokumentací,
- srovnávání nebo modelování.



- Analýza probíhá vyhodnocením stavu z hlediska rizik. Tvoří hlavní fázi celého procesu. Kvalita analýzy rizik určuje platnost závěrů a doporučení.
- Doporučení pak obsahuje návrh protiopatření pro optimalizaci rizik.

0





Formy bezpečnostní kontroly

- Bezpečnostní kontrola může mít několik forem a můžeme ji dělit například dle:
 - **časového kritéria**
 - plánovanou,
 - mimořádnou a
 - následnou kontrolu
 - **věcného kritéria**
 - komplexní nebo
 - dílčí.

0





Legislativa

- Při zpracování návrhu bezpečnostní strategie organizace musíme klást důraz mimo výsledků analýzy rizik také na požadavky, které vyplývají z platné legislativy.
- Pojem bezpečnost organizace zahrnuje široké spektrum oblastí napříč firmou, kterých se dotýká a která musí být legislativně ošetřena.
 - Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů v platném znění,
 - Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů v platném znění,
 - Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů v platném znění,
 - Zákon č. 106/1999 Sb. o svobodném přístupu k informacím v platném znění,
 - Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění,
 - Zákon č. 262/2006 Sb. Zákoník práce,
 - Zákon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci,
 - Zákon č. 133/1985 Sb., o požární ochraně.
 - Zákon 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), změn 104/2017 Sb., 183/2017 Sb., 205/2017 Sb.





Normy

- V mezinárodní normě ISO/IEC 17799 je uvedena specifikace požadavků na systém řízení v oblasti bezpečnosti informací.
- Jde o stěžejní normu pro zavádění a certifikaci systémů řízení organizace. Systém managementu bezpečnosti informací je uveden v Normě BS 7799-2.
- Norma ČSN ISO/IEC 27001 stanoví požadavky na systém managementu bezpečnosti in-formací tak, aby byla organizace schopna vyhodnocovat svá rizika a uplatňovat náležité kontrolní a řídicí mechanismy k zachování důvěrnosti, integrity a dostupnosti informací.
- Norma ČSN ISO/IEC 15408 se týká informačních technologií, bezpečnostní techniky a kritérií pro hodnocení bezpečnosti IT.
- Norem týkajících se bezpečnosti je celá řada, mezi další důležité patří také Norma ČSN EN 5 130, týkající se poplachových systémů a mnohé další.

0





Výhody a nevýhody použití norem při zajištění bezpečnosti

- Standardy vytvářejí vzor řešení určitého problému, není tedy nutné dané problémy řešit vždy znovu. Tím se šetří čas i prostředky.
- Pokud se problémy řeší pomocí stejného standardu, povaha výsledků je vždy stejná, a je tak možné je sdílet, nebo používat stejným způsobem.
- K výhodám užívání norem v organizaci patří zejména sjednocení provedení výrobků, zajištění vyměnitelnosti součástí na strojích při opotřebování nebo poškození, zvýšení sériovosti, hromadnosti a plynulosti výroby, čímž se přispívá k její zrychlení a zlevnění.
- Další výhodou je bezesporu zhuštění výroby a snížení ceny výrobků, zjednotění způsobů provádění výpočtů, projektování, konstruování a metody zkoušení materiálů a výrobků.
- Normy též pomohou zjednotit značky, symboly nebo názvy jednotek. Za nevýhody můžeme označit to, že standardizace omezuje uživatele na předem dané postupy a případy určené standardem.
- Standardizací není možné postihnout všechny možné případy. Vývoj a udržování standardu vyžaduje financování a někdo je tedy musí hradit. Standardy mohou být předmětem patentů a za jejich používání je nutné platit licenční poplatky





Bezpečnostní management

- Cílem bezpečnostního managementu je správa bezpečnosti v organizaci, zajišťující její požadovaný stav.
- Přijímaná bezpečnostní opatření musí být cílená.
- Opatření můžeme rozdělit na preventivní a represivní.
 - Cílem preventivních opatření je působit proti příčinám, řešit příčiny expozice bezpečnostních hrozeb.
 - Represivní opatření nastupují v případě akutní možnosti expozice bezpečnostních hrozeb a při jejich expozici. Represivní opatření působí vůči škodícímu účinku, brání vzniku újmy nebo alespoň zmírňují její velikost.

0





Bezpečnostní management

- Pro konkrétní obsah bezpečnostního managementu je důležité provést potřebnou analýzu rizik, potřeb zajištění bezpečnosti a z toho vyvodit odpovídající požadavky na bezpečnostní management.
- Významný vliv na charakter bezpečnostního managementu bude mít i to, jedná-li se o bezpečnost vůči záměrným nebo nezáměrným hrozbám.
- Zabezpečení vůči záměrným hrozbám vyžaduje silové působení a trvalou připravenost. Při zabezpečení vůči nezáměrným hrozbám je kladen důraz na kontrolu stavu a podmínek, dodržování pravidel i připravenost ochranných opatření.

0





Bezpečnostní management

Mezi základní požadavky na bezpečnostní systém a tím i zprostředkovaně bezpečnostní management patří:

- připravenost
- reakce-schopnost
- adekvátnost
- vytrvalost
- pružnost
- řiditelnost
- ekonomická efektivnost

0





Oblasti bezpečnostní strategie organizace

- Bezpečnostní strategii organizace mohou tvořit zejména následující oblasti:
 - fyzická bezpečnost,
 - informační bezpečnost,
 - administrativní bezpečnost
 - bezpečnost KIS
 - kryptografická ochrana
 - personální bezpečnost,
 - bezpečnost a ochrana zdraví při práci,
 - požární ochrana.

0





Závěrem k bezpečnostní strategii firmy

- Obsahem je zejména stanovení cílů a popis způsobu zajištění celkové bezpečnosti informačního systému ve vztahu k bezpečnosti organizace.
- Je to výběr bezpečnostních zásad a předpisů splňující bezpečnostní politiku organizace a všeobecně definujících bezpečné používání systémů v rámci organizace.

0





Závěrem k bezpečnostní strategii firmy

- Jedná se tedy o detailní normy, pravidla, praktiky, předpisy konkrétně definující způsob zajištění bezpečnosti organizace.
- Dokumenty celkové bezpečnostní strategie by měly být předloženy zaměstnancům organizace a to ve formě, která je relevantní, přístupná a pochopitelná.

0





Závěrem k bezpečnostní strategii firmy

- Praktické zavedení jednotlivých opatření do každodenního provozu fungující organizace vždy přináší určité restrikce vůči zaměstnancům a klade na ně požadavky, na něž dosud nebyli zvyklí.
- Zatímco restriktivní složka těchto opatření je patrná hned a pracovník ji pocítí s okamžitou platností, přínos daných opatření už tak snadno a jasně vidět není a obvykle se projeví až po určitém časovém úseku.

0





Závěrem k bezpečnostní strategii firmy

- Je lidské se všem změnám bránit, a tak je prosazení nových opatření a zavádění nových struktur nesnadný úkol.

0





Závěrem k bezpečnostní strategii firmy

- Zodpovědní pracovníci by měli mít v zásobě velkou dávku:
 - trpělivosti,
 - asertivity a
 - znalosti lidských vztahů.

0





Samostudium otázky

- Definujte význam pojmu kauzalita.
- Jaký je rozdíl mezi induktivním deduktivním přístupem při zkoumání kauzality?
- Objasněte metody kauzální analýzy.

0





Literatura

- LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management V . Zlín: Radim Bačuvčík - VerBuM, 2015. ISBN 978-80-87500-67-5.
- Bezpečnostní strategie ČR [online]. Praha: Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR, 2015 [cit. 2016-05-12]. Dostupné z: <http://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie2015.pdf>
- ADAMEC, Vilém, David ŘEHÁK a Lenka ČERNÁ. Základy organizace a řízení bezpečnosti v České republice . 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2012. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-123-1.
- NOVÁK, Jaromír. Vnitřní a vnější bezpečnost státu . 1. vyd. V Olomouci: Univerzita Palackého, 2014. ISBN 978-80-244-4371-3. [12] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích . 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80247-4644-9.
- PEXIDR, Karel a Nikolaj DEMJANČUK. Kauzalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009. ISBN 978-80-7380-128-1.
- MLEZIVA, Emil. Diktatura informací: jak s námi informace manipulují. Plzeň: Aleš Čeněk, 2004. ISBN 80-86898-12-1.
- JANOŠEC, Josef. Hrozba a riziko v bezpečnostní terminologii. Lázně Bohdaneč: Ministerstvo vnitra, 2010.

